CSIT Conference 2021, Yerevan, Armenia, September 27 - October 1

Comparative Analysis of Modern E-Voting Systems Based on Security Criteria

Arman Avetisyan
Russian-Armenian University
Yerevan, Armenia
email: armanavetisyan1997@gmail.com

***Abstract*—This paper provides a comparative analysis of modern electronic voting systems based on security criteria. The development of reliable and safe e-voting systems is relevant because of the wide range of applications . A comparative analysis was conducted on the most popular modern e-voting systems used in several countries to point out strengths and weaknesses of each one. The comparison gives better understanding of the current state of those systems and can be used in creating a more secure and reliable e-voting system.**

***Keywords*— Electornic voting, information security, elections, secure voting.**

I. Introduction

Electronic voting(e-voting) is a term that encompasses several different types of voting methods and electronic means of counting votes. E-voting systems include punched cards, optical voting systems and specialized voting kiosks (including stand-alone electronic systems for direct voting), and means for the transmission of ballots and votes by telephone, via the private computer network or via the Internet. Such systems would speed up the counting of votes and make voting more accessible and transparent. However, weak e-voting systems could encourage electoral fraud. The advantages and disadvantages of modern E-voting solutions and technologies should be explored in order to create a secure system. This study focuses on the electronic systems through which the entire electoral process (voter registration, voting and counting votes) is conducted. The study distinguishes the standard functionality of e-voting systems[1-2].

Standard e-voting systems include the following modules:

- electronic voter lists and a method of voter identification,
- interface for polling station staff,
- interface for voters,
- system for sending votes to count,
- interface to show results.

The e-voting system should correspond to a series of criteria, which can be divided into two important groups, primary - based on security and safety of the system, and secondary - based on user friendliness and accessibility.

System safety requirements are:

- integrity of elections,
- privacy of the vote,
- authenticity of the voters,
- verifiability of the votes,
- protection against attacks,
- ensuring the confidentiality of personal data.

At the international level, the systems developed and tested today have some security problems. A great deal of scientific literature has been devoted to this study, but a number of questions remain[1,3-6]. Even the best e-voting systems this day have some drawbacks. The study reviews electoral systems in some countries, where e-voting was used during elections. The comparative analysis is carried out on the basis of the basic safety criteria, based on the abundant literature available. The results of the comparative analysis are shown in a table that provides a complete picture and a clear understanding of the advantages and limitations of modern e-voting systems.

II. E-voting systems

A. How e-voting systems work

Research has been active in the last twenty years to create secure voting systems. These systems are based on public key cryptographic systems and the approach that the voter's vote is encrypted with a public key that corresponds to it. The private key is distributed among the members of the electoral commission, so the members of the electoral commission will be able to decrypt and count the votes together. In addition, to ensure the secrecy of the ballots special methods are used (MIX network, additive homomorphic encryption systems...)[7-8]. The initial systems were based on the assumption that each voter has sufficient amount of technical skills and can perform complex operations like encryption on their own. This approach was of theoretical interest and could not be applied to create voting systems because the majority of voters do not have technical skills, so those systems cannot be considered reliable in elections.

After 2000, two main directions began to appear in election systems: e-voting using special ballots for on-site voting, and internet voting using personal computers to send the vote via internet. The latter is undoubtedly more convenient but study

has shown that reliability of internet voting can be lacking due to personal computers not being secure enough. If the person wants to vote for candidate X and tells the computer to do so, the connection might be intercepted and a vote for candidate Y may be sent instead. Many internet voting protocols have been proposed since then to use for elections in different countries (like Norway, where e-voting have been used exclusively) which will be analyzed in Section 3.

All voting systems must have the following phases[2]:

- **Setup phase.** Parameters of election are formed and publicized. Those parameters include encryption keys, number of candidates, voter lists, etc.
- **Ballot filling phase.** During this phase, the voters prepare their vote with a special ballot or personal computer. The result should be a ballot or e-ballot with voter's personal info embedded in it.
- **Ballot registration phase.** The ballot with embedded info and voter's personal number are sent to public ballot storage.
- **Ballot anonymity phase.** Voter's info is removed from the ballot, which is then encoded and as a result a ballot without voter info is collected. The authenticity of the ballot can be checked via private keys that are only given to election committee.
- **Counting phase.** The committee uses the private key parts in their possession to create the complete key to decode all the ballots and count the votes.

B. Closer look at the security criteria of e-voting systems

Numerous security criteria have been proposed for e-voting systems, some of which are mandatory for all systems, some may be mandatory only during special elections. Let's take a closer look at the most importants of them[9-11].

1. Integrity of elections. Ensuring the accuracy of elections is the main and most important criteria, without it, the system is unusable. The criteria are broken down into 3 parts.

- **Accuracy:** ensuring that all registered ballots are accurate. This means that all the ballots that are to be counted are sent by eligible voters for competing candidates.
- **Completeness:** all the ballots are counted, no ballot is ignored or erased.
- **Stability:** no ballot is subject to change after being sent to ballot storage.

It is evident that without these basic principles, fair elections cannot be organized, thus making Integrity the essential criteria for any system.

2. Privacy of the vote. When it comes to paper ballots, privacy of the votes is kept by making all the ballots visually the same and thus indistinguishable inside the ballot box. It is harder to keep the privacy in e-voting systems. In modern systems only the whole committee or sometimes a coalition in the committee is able to decode the ballot to uncover a voter's ballot. This means that in modern e-voting systems, if everyone in the committee is working together, it is possible to violate the privacy of the voters.

3. Authenticity of the voters. Authenticity of the voters means that only eligible voters can cast a vote and that they can do it only once. To ensure this the system must have a module that will authenticate and register the voters. Usually, a government-issued ID is used for this but some systems use cryptographic methods like an electronic signature.

4. Verifiability of the voter. Verifiability is a criterion that gives e-voting an advantage over regular methods of voting. It means that anyone can check to see if their vote was counted in the elections as well as see if it was changed or not. To ensure verifiability the voter must be able to check the integrity of their ballot during all 3 of the following phases: when they register to vote, when they send their ballot and when their ballot is counted. If fraud is commited, verifiability of the system is responsible of alerting a person and the committee.

5. Protection against attacks This criteria ensures that each vote cannot be tampered with. It is largely connected to the secrecy of the vote, if the information about the vote is not accessible, it cannot be changed. The system should also be secure against attacks that are commited before the vote is cast, for example if the attacker makes it impossible to cast a vote or makes the voter vote for the wrong candidate. In both cases, if given enough information, the voter should be able to spot the tampering and report it to the system.

6. Ensuring the confidentiality of personal data. Ensuring the confidentiality of personal data means that no one, even the voter cannot prove who they have voted for. This means that confidentiality is not done for the voter but for the security of the system and lowering the rate of common election frauds such as bribes.

These are the main security criteria that portray an ideal voting system. In the next section we will take a look at modern e-voting systems and provide a comparative analysis of their advantages and disadvantages.

III. Analysis of e-voting systems in different countries

In this section, we will take a look at e-voting systems that have been used for various elections in different countries and analyze them in terms of criteria given in Section 1.

Norway. In 2011 Norway held local elections using a cryptographic e-voting system developed by SCYTL. This system uses paper ballots, but it was one of the first instances of keeping the connection between the voter and the system using external communications, in this case it was sms messages. One of the main flaws of this system is that anyone that can get their hands on a receipt provided by the system can tell who the voter voted for, which is a violation of privacy criteria. This also makes the system vulnerable to attacks as a lot of

Country	Integrity	Privacy	Authenticity	Verifiability	Protection	Confidentiality
Norway	✔	✘	✔	✘	✔✘	✔
USA	✔	✘	✔	✔	✔✘	✘
Netherlands	✘✔	✘	✘	✘	✘	✘
Brazil	✔	✔	✔	✘	✘	✘
Estonia	✘✔	✔	✔	✔	✘	✔
Canada	✔	✔	✔	✘	✘	✘

TABLE I
COMPARATIVE ANALYSIS OF DIFFERENT COUNTRIES' E-VOTING SYSTEMS, BASED ON SECURITY CRITERIA

faith is being put in voter's ability to protect their information themselves. It has been noted by many observers that client-side security of the system still remains lacking, so it is more prone to attacks during the voting process. More info about this system is given in[12-13].

USA. Scantegrity II e-voting system was used in 2009 in USA for municipal elections. This system uses paper ballots, which are scanned after voting and then processed digitally. Cryptographic methods are used to generate and count ballots. The scanners used in this system are vulnerable to attacks, usage of paper ballots greatly reduces the safety of voter data, and generation of needed cryptographic methods assumes the existence of a trusted third party, so the privacy and confidentiality of user information still remains a problem for US voters[14-16].

Netherlands. E-voting in the Netherlands started to be discussed as early as 2006. Several experiments have been conducted, including the possibility of voting over internet, but ultimately all systems have been rejected because of public distrust and unreliability of those e-voting systems. As to the systems mentioned above, e-voting systems in the Netherlands used paper ballots for elections, created via specialized ballot printers, but designing and testing a sufficiently protected ballot printer was judged to be infeasible for any practical election process. The systems designed were practically helpless against external threats, which led to public distrust and ultimate abolishment of e-voting in the Netherlands. As the system did not meet the required safety criteria, the Netherlands government decided not to turn back to paper-based manual voting and counting[17-18].

Brazil. Currently, in Brazil, all votes are cast by e-voting machines.In 2000, the Brazilian government had converted to fully e-voting and deployed over 400,000 kiosk-style machines in elections that year. This machines are quite unusual as they tally the votes once voting finishes producing digital and paper report of the number of votes. After the vote the machine prints out a ballot for the voter to put in a box to be counted in case of a recount. These paper-trail machines were successfully used during the election in Brazil but they still heavily rely on paper voting and cannot act as a standalone system. Paper-based voting system and the unusual structure of voting machines cause many vulnerabilities during elections, which is a reason for concern. Another major concern in Brazil elections is the ability for poll station workers to vote for absentees, by acquiring needed voter data, which is easy to obtain due to insecurities within the system, recently a biometric verification requirement was put in place but the vulnerability within the system still remains intact[19-20].

Estonia. Estonia introduced e-voting systems for their elections as early as 2003 and since then have steadily improved the quality of those systems.The most notable change is heavier leaning into internet voting, which is still considered insecure by many security experts.Studies have shown that even though the system itself is quite reliable, Estonian e-voting relies on insecure public channels to send information about the vote. In 2014, a team of security experts claimed that they can breach the Estonian system, change or erase votes, but no substantial changes have been made to the system since then. Estonian e-voting system is considered one of the best in terms of security nowadays and is widely used, understanding the problems of this system will undoubtedly help to build a more secure and reliable system that can be widely used. The concern about integrity of the system arose when computer experts claimed that the system which transmitted ballots was rather insecure and prone to attacks, thus endangering the integrity of the ballots. Upon review the Estonian National Election Committee claimed that there was no need to temporarily suspend the use of internet ballots, raising a controversy between National Information System Authority and independent researchers[21-24].

Canada. An internet voting system is used for over 60 municipality elections in Canada. The system was evaluated in Internet voting known as 2012 Jellybean internet voting election. Although the system showed outstanding results in user experience, availability and general user-friendliness, many flaws were identified in the security part of the system, such as unreliable verifiability of the vote and low evaluations of robustness and safety of voting. Based on the test results, Canadian officials decided not to introduce the system for General Elections[25].

It is evident that the main problem of modern e-voting systems is protection against attacks during voting, counting and especially while transmitting the votes. The issue of creating a sufficiently secure system is widely discussed nowadays. A lot of propositions include creating a secure channel for ballot transmissions, because that's the problem that can be solved technologically, voters would always be at risk of human error during voting, but having a secure communication between the voting device and the system is crucial to lowering the risk of fraud[26-30]. The main idea that is discussed today is using cryptography and blockchain to have a secure channel between the device and the system, which require entirely

new and questionable security protocols. These techniques may undoubtedly be helpful for secrecy but they don't address several security issues of e-voting discussed in[31].

IV. Conclusion and future work

A comparative analysis of various e-voting systems based on security criteria have been conducted. The main problems of modern voting systems are the need for paper ballots, which make systems vulnerable to human error, and usage of insecure communication channels to send voter data, which make the system vulnerable to external threats. One of the main problems of creating reliable e-voting systems is designing a secure infrastructure for all stages of elections, thus getting rid of human factors. Based on the analysis, we can conclude that modern systems are not secure against external attacks, and this should be the main area of focus in newer systems. This can serve as a basis for creating more secure e-voting systems in the future, which are based on the systems used today but will have an added layer of protection, e.g., a stenographic system for the security of the public channel, storage and transfer of critical information during an election.

References

[1] Stenbro M. *"Survey of Modern Electronic Voting Technologies"*, NTNU, June 2010.

[2] International IDEA *"Introducing Electronic Voting: Essential Considerations"*, (https://www.corteidh.or.cr/tablas/28047.pdf), 2011.

[3] K. Krips, J. Willemson, S. Varv, "Is your vote overheard? a new scalable sidechannel attack against paper voting", *Proceedings of Euro SP 2019*, pp. 621– 634. IEEE 2019.

[4] A. S. Neto, M. Leite, R. Araujo, M. P. Mota, N. C. S. Neto, J. Traore, "Usability considerations for coercion-resistant election systems", *Proceedings of the 17th Brazilian Symposium on Human Factors in Computing Systems*, pp. 40:1–40:10 2018.

[5] P. Y. A. Ryan, P. B. Rønne, V. Iovino, "Selene: voting with transparent verifiability and coercion-mitigation", *Lecture Notes in Computer Science*, vol. 9604, pp. 176–192. Springer, Heidelberg 2016.

[6] J. Willemson, "Bits or paper: which should get to carry your vote?", *Journal of Information Security and Applications*, pp. 124–131, 2018.

[7] J. Benaloh, D. Tuinstra. *"Receipt-free secret-ballot elections"*, STOC'94, pp 544–553, USA, 1994.

[8] D. Wikstrom, J. Groth, "An adaptively secure mix-net without erasures", *Lecture Notes in Computer Science*, vol. 4052, pp. 276–287. Springer, 2006.

[9] K. M. AboSamra, A. A. AbdelHafez, G. M.R. Assassa, M. F. M. Mursi, "A practical, secure, and auditable e-voting system", *Journal of Information Security and Applications*, vol. 36, pp. 69–89, 2017.

[10] A. Driza Maurer, *"Updated European Standards for E-voting"* Electronic Voting. E-Vote-ID, 2017.

[11] S. A. Adeshina, A. Ojo, *"Design imperatives for e-voting as a sociotechnical system"* 2014 11th International Conference on Electronics, Computer and Computation (ICECCO), 2014.

[12] J. i Esteve, B. Goldsmith, J. Turner, *"International Experience with E-Voting, Norwegian E-Vote Project"*, no. June, pp. 1–196, 2012.

[13] M. J. M. Chowdhury, "Comparison of e-voting schemes: Estonian and Norwegian solutions", *International Journal of Applied Information Systems*, vol. 6, no. 2, pp. 47–54, 2013.

[14] K. Sanjay, "Analysis of electronic voting system in various countries", *International Journal on Computer Science and Engineering*, May 2011.

[15] P. S. Herrnson, R. G. Niemi, M. J. Hanmer, B. B. Bederson, F. G. Conrad, M. W. Traugott, "The Current State of Electronic Voting in the United States", *Digital Government. Integrated Series In Information Systems*, vol. 17, 2008.

[16] G. Dave, *"Introducing biometrics in the U.S. voting process"*. https://www.biometricupdate.com/201610/introducingbiometrics-in-the-u-s-voting-process-qa-with-dave-gerulski, 2016.

[17] L. Loeber, "The E-voting Readiness Index and the Netherlands", *Electronic Voting. E-Vote-ID 2018. Lecture Notes in Computer Science*, vol. 11143, 2018.

[18] L. Loeber, "E-Voting in the Netherlands: from General Acceptance to General Doubt in Two Years", *3rd International Conference on Electronic Voting*, vol. c, pp. 21–30, 2008.

[19] D. F. Aranha, J. van de Graaf, "The Good, the Bad, and the Ugly: Two Decades of E-Voting in Brazil", *IEEE Security Privacy*, vol. 16, no. 6, pp. 22-30, Nov.-Dec. 2018.

[20] M. Hapsara, A. Imran, T. Turner, "E-Voting in Developing Countries.", *Electronic Voting. E-Vote-ID 2016. Lecture Notes in Computer Science*, vol. 10141, 2017.

[21] E. Estonia, *"Internet Voting in Estonia, e-Estonia the Digital Society"*, Online at: http://e-estonia.com/components/i-voting, 2012.

[22] W. Drechsler, Ü. Madise, "E-VOTING IN ESTONIA", *TRAMES*, 6(56/51), 3, pp. 234–244, 2002.

[23] AG. Tsahkna, "E-voting: lessons from Estonia", *European View 12*, https://doi.org/10.1007/s12290-013-0261-7, 2013.

[24] E. Estonia, *"Internet Voting in Estonia, e-Estonia the Digital Society"*, Online at: http://e-estonia.com/components/i-voting, 2012.

[25] N. Goodman, J.H. Pammett, J. De Bardeleben, *"A comparative assessment of electronic voting"*, Report Prepared for Elections Canada, 2010.

[26] V. Martin, "Evaluation of Internet Voting Systems based on Requirements Satisfaction", *International Review of Social Sciences and Humanities*, vol. 6, no. 1, pp. 41-52, 2013.

[27] V. Cortier, C. Wiedling, "A formal analysis of the Norwegian e-voting protocol", *Lecture Notes in Computer Science*, vol. 7215, pp. 109-128, 2012.

[28] A. T. Sherman, R. A. Fink, R. Carback, D. Chaum, "Scantegrity III: Automatic trustworthy receipts, highlighting over/under votes, and full voter verifiability", *Proceedings of the Electronic Voting Technology/Wokrshop on Trustworthy Elections*, EVT/WOTE, 2011.

[29] B. Jacobs, W. Pieters, "Electronic Voting in the Netherlands: from early Adoption to early Abolishment", *Foundations of Security Analysis and Design V: FOSAD 2007/2008/2009 Tutorial Lectures*, pp. 121-144, 2009.

[30] Sarah P. Everett, Kristen K. Greene, Michael D. Byrne, Dan S. Wallach, Kyle Derr, Daniel Sandler, Ted Torous, "Electronic Voting Machines versus Traditional Methods: Improved Preference, Similar Performance", *Proceedings of Measuring, Business and Voting*, Florence, Italy, April 5-10, 2008.

[31] Sunoo Park, Michael Specter, Neha Narula, Ronald L. Rivest, "Going from bad to worse: from Internet voting to blockchain voting", *Journal of Cybersecurity*, vol. 7, iss. 1, 2021.